Department of Homeland Security Daily Open Source Infrastructure Report for 19 August 2005

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Journal News reports a committee of transportation advocates says the New York Metropolitan Transportation Authority and its transit divisions must refine their emergency communications plans to keep passengers and employees safe during a terrorist attack or other emergency. (See item 9)
- Agence France−Presse reports Vancouver International Airport will become the first in the world to operate a new radar system that can detect the smallest piece of debris on a runway with pinpoint accuracy. (See item 11)
- The Associated Press reports the U.S. Department of Agriculture has said that its testing options for mad cow disease were limited in 9,200 cases despite its effort to expand surveillance throughout the U.S. herd. (See item 18)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 18, Angus Reid Global Scan* — **Support for nuclear power grows in U.S.** More adults in the United States believe the country should build new atomic reactors, according to a poll by Rasmussen Reports. Fifty−five percent of respondents think it is time to begin building

nuclear power plants again, up 11 points since June. Sixty−four percent of respondents believe developing new power sources is more important in the long run, while 26 percent favor conservation. More than 100 nuclear reactors supply close to 20 percent of the electricity used in the U.S. In May, the nuclear power consortium NuStart Energy named six sites in Alabama, Louisiana, Maryland, Mississippi, New York and South Carolina as prospective locations for future power plants.
More poll information: http://www.rasmussenreports.com/2005/Energy_Nuclear%20Power_August%2016.htm
Source: http://www.angus−reid.com/polls/index.cfm/fuseaction/viewIte m/itemID/8567

2. *August 17, Associated Press* — **Cooler weather won't curb energy problems.** After a summer of soaring gasoline costs, people should not expect cooler weather in autumn to end their energy woes. Prices at the gas pump probably will stay high and record heating bills in the winter are almost certain to follow. The Department of Energy predicts that heating costs for homes using natural gas or fuel oil could be 16 percent to 25 percent higher than last year. Utilities are warning customers that their bills will be high this winter, says Chris McGill of the American Gas Association, which represents the natural gas retailers. Wholesale prices for natural gas have soared along with crude oil and gasoline. The Energy Information Administration estimates that natural gas could cost more than $10 per thousand cubic feet by January, about 30 percent more it did this summer. A little more than half of U.S. homes use natural gas for heating; the heaviest concentration is in the Midwest.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/08/17/AR2005081701392.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *August 18, Bristol Press (CT)* — **Collision causes diesel spill on Connecticut road; area briefly evacuated and traffic rerouted.** In Bristol, CT, a two−vehicle accident occurred at Middle Street and Redstone Hill Road in which the fuel tank of a tractor−trailer truck was ruptured, causing a brief evacuation of the area and traffic to be rerouted Wednesday evening, August 17, according to police Sergeant Richard Valentine. Emergency personnel quickly discovered the fuel to be diesel and called off the evacuation, he said. Valentine said that based on the initial report of leaking fuel, police and firefighters began evacuating the area and called in the state Department of Environmental Protection (DEP) as a precautionary measure. Because of the fuel spill, DEP workers and specially trained Hazmat crews responded to the scene.
Source: http://www.bristolpress.com/site/news.cfm?newsid=15055493&BRD=1643&PAG=461&dept_id=10486&rfi=6

4. *August 18, NBC 11 (CA)* — **Hazmat spill closes California highway.** A shelter−in−place order is in effect for South Bay, CA, residents in the area of a sulfuric acid spill, which has forced the closure of both directions of U.S. Highway 101 at Blossom Hill Road and Bernal Road. California Highway Patrol (CHP) units were at the scene, where it is believed between 500−800 gallons of sulfuric acid spilled from a tractor−trailer onto the freeway, said CHP spokesperson Wayne Ziese. The driver of the truck was taken to a hospital with burns on his

face. Ziese advised residents who live near the area of the spill to stay inside and keep windows and doors closed. Traffic on U.S. Highway 101 in San Jose, CA, is being diverted to alternate routes. All lanes of the highway between state Highway 85 and Blossom Hill Road are closed indefinitely, according to the CHP.
Source: http://www.msnbc.msn.com/id/8998793/

5. *August 17, NBC 4 (TX)* — **Neighborhood evacuated in Texas after plant fire, no injuries.** Investigators with the Occupational Safety and Health Administration (OSHA) went to Borger, TX, Thursday, August 18, to investigate what caused a fire to break out at the Chevron−Phillips Ryton plant late Tuesday, August 16. It began about 9 p.m. and was under control two hours later. Because the plant contains a lot of chemicals, the Borger Fire Department evacuated a neighborhood as a precaution. No one was injured. A Chevron−Phillips plant manager says the public was never in danger.
Source: http://66.228.51.10/news/default.asp?mode=shownews&id=870

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

6. *August 18, Government Computer News* — **Users succumbing to targeted phishing, experts say.** Internal security exercises conducted by the U.S. Military Academy at West Point and New York State's chief information security officer (CISO) found that many e−mail recipients fall for phishing scams that appear to have been sent from within their organizations. Educating and testing e−mail users have limited success, according to Aaron Ferguson, visiting faculty member at West Point and a system engineering manager at the National Security Agency. "We got an 80 percent click rate," on the first test e−mail, sent to 400 West Point cadets, Ferguson said. Subsequent exercises with as many as 3,000 cadets produced lower response rates, but the rates did not drop sharply, he said. New York state CISO Will Pelgrin reported similar findings in tests of 10,000 state employees in five departments. The New York State and West Point exercises were carried out to test the effectiveness of awareness programs. E−mail supposedly from officials within an organization apparently had a high level of credibility. The West Point test was especially effective because it bore the name of a colonel, Ferguson said. When you get an order from a colonel, he said, "You execute the order and ask questions later."
Source: http://www.gcn.com/vol1_no1/daily−updates/36692−1.html

7. *August 18, InformationWeek* — **Consumers concerned about online security.** The string of customer−data security lapses this year has exacerbated consumer tensions about online security, according to a survey released Thursday, August 18, by RSA Security Inc. and LightSpeed Research. More than four−fifths of 8,000 consumers surveyed reported feeling threatened or extremely threatened by online fraud and identity theft. The fears extended across all types of online transactions, including securities trading, banking, auctions, and retail. The

survey was taken in May as reports of incidents involving lost data tapes, customer−data breaches, and system hacking were reaching a peak. Consumers are taking information security into account when considering financial−services providers; 45% of respondents said they'd be more likely to switch brands if a new provider offered a stronger authentication method. Businesses, which tend to be tight−lipped about their security practices, should be more forthcoming in the interest of alleviating consumer concerns, says Orson Swindle, a former member of the Federal Trade Commission. "Companies need to tell their stories about what they're doing and how much they're spending on information security," he says.
More survey information: http://www.rsasecurity.com/press_release.asp?doc_id=6010
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=QHNJND24A1HTWQSNDBCCKHSCJUMEKJVN?articleID=169400081

8. *August 18, IDG News Service* — **Finnish officials urge better Wi−Fi security after bank break in.** It emerged this week that about $245,400 had been stolen from a Finnish bank using an unprotected home network. The Helsinki branch of global financing company GE Money called on police to investigate the theft in June. The money, which has since been recovered, was stolen from one of GE Money's accounts at a local bank, said Jukkapekka Risu, investigating officer for the Helsinki police. Police now believe that the company's 26−year−old head of data security in Helsinki stole banking software from the company along with passwords for its bank account, Risu said. Accomplices then accessed the account from a laptop computer using an unprotected network from a nearby apartment building. They used the passwords to transfer the money to a different corporate account that they had set up six months earlier, Risu said. Police declined to name the suspects or identify the bank from which the money was stolen. Risu called it a "large, local bank." The case has prompted the Finnish Communications Regulatory Authority to remind citizens about the dangers of not securing their wireless networks.
Source: http://www.infoworld.com/article/05/08/18/HNfinnwifisecurity_1.html

[Return to top]

Transportation and Border Security Sector

9. *August 18, Journal News (NY)* — **Review finds gaps in transit emergency procedures.** A New York state committee of transportation advocates said on Wednesday, August 17, that the Metropolitan Transportation Authority (MTA) and its transit divisions must refine their emergency communications plans to keep passengers and employees safe during a terrorist attack or other emergency. In its report, "Ladies and Gentlemen: This Is Not A Drill," the Permanent Citizens Advisory Committee to the MTA praised Metro−North Railroad for its emergency communications system and employee training. However, it sharply criticized the MTA, New York City Transit (NYC Transit) and Long Island Rail Road (LIRR) for inadequate emergency communication plans and for not clearly outlining employee responsibilities in the event of a crisis. The review also found that NYC Transit and LIRR did not have formal emergency task forces to develop strategies and did not regularly review and update existing plans. In a letter sent to Beverly Dolinsky, the advisory committee's executive director, MTA officials called some research in the report "outdated." Katherine Lapp, the MTA's executive director, wrote that the agency's Website has been revised to provide the public with more information and that regular reviews of emergency plans was an already established policy.

Report: http://www.pcac.org/
Source: http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20050818/NEWS02/508180343/1017

10. *August 18, Associated Press* — **French experts join Venezuela plane crash probe.** French specialists joined an investigation into the crash of an airliner that killed 160 people, while Colombia grounded the airline that offered the charter flight to vacationers from the French Caribbean island of Martinique. The Colombian government said late Wednesday, August 17, it had halted West Caribbean Airways' operations while its civil air authority reviewed inspections that the small carrier had been required to perform. The Colombian airline's safety record is being scrutinized after the McDonnell Douglas MD−82 crashed in Venezuela Tuesday, August 16, while bringing passengers home to Martinique after a weeklong trip to Panama. Venezuelan investigators were focusing on the possibility of contaminated fuel or some other fuel problem that led both engines to fail simultaneously, said Nelson Serrano, an emergency official in the western state of Zulia. "The one thing that can cause an engine like that to have a problem is fuel contamination," said Paul Czysz, emeritus professor of aerospace engineering at St. Louis University in the United States. Panamanian authorities, however, said they found no evidence of tainted fuel and that the plane had plenty of fuel for the trip. The pilot radioed the nearest airport before the crash, saying both engines had failed.
Source: http://www.usatoday.com/news/world/2005−08−18−venezuela−cras h_x.htm

11. *August 18, Agence France−Presse* — **New airport radar will help avoid repeat of Concorde crash.** Vancouver International Airport will next year become the first in the world to operate a new radar system that can detect the smallest piece of debris on a runway with pinpoint accuracy, officials said. The airport, on Canada's west coast, has bought four Tarsier radar units developed by British company QinetiQ following the Concorde crash at Paris Charles de Gaulle airport in July 2000, which killed 113 people. The disaster was blamed on a piece of metal that fell of another passenger jet, punctured a tire and caused secondary damage. The Tarsier, based on high−resolution millimeter wave radar, is able to detect material the size of a 2−inch bolt to within 10 feet, at a range of up to 1.5 miles. It can also tell if the item is made of metal, plastic, glass, wood or animal remains. Once computer software identifies the item, a global positioning system is used to direct airport staff to its location to clean up the debris, he said. Currently, checking for debris is done manually −− staff walk up and down runways with a broom and a dustpan. Prone to human error, the method is also time consuming and expensive if it delays incoming or outgoing flights, Richmond said.
Source: http://www.usatoday.com/travel/news/2005−08−18−airport−radar_x.htm

12. *August 18, Associated Press* — **Controllers say understaffing caused planes to fly too close.** Air traffic controllers claim severe staffing shortages are to blame for a series of mistakes, including two in the last five days, that caused planes to fly dangerously close to one another over California. The Federal Aviation Administration (FAA) says the close calls resulted from human error unrelated to working conditions. "Neither of those had anything to do with staffing" at the Palmdale air traffic control center that handles high−altitude aircraft in Southern California and parts of Arizona, Nevada and Utah, FAA spokesperson Donn Walker said Wednesday, August 17. Understaffing means greater workloads, longer work hours and fewer eyes available to catch mistakes, claims Hamid Ghaffari, the National Air Traffic Controllers Association representative for Los Angeles Center in Palmdale, CA. Both of the recent close

calls, which occurred during bad weather, resulted from controller mistakes, he said. Nine such errors have occurred during the past two months and 27 since October 1, he said. The control center is authorized to employ 310 controllers but has just 217 certified personnel and 48 trainees, including 21 who can do very little because they're brand new to the job, Ghaffari said.
Source: http://www.usatoday.com/travel/flights/2005−08−17−understaff ing_x.htm

13. *August 18, Associated Press* — **Dallas airport will use federal grant on taxiways.** Dallas−Fort Worth International Airport (DFW) plans to use a $4 million federal grant to build perimeter lanes that will let planes taxi around the airfield without crossing runways. Officials said the new ribbons of concrete would improve safety and get passengers to the gate faster at DFW, the world's third busiest airport, with nearly 2,000 flights a day, according to airport officials.
Airport Website: http://www.dfwairport.com
Source: http://www.dentonrc.com/sharedcontent/APStories/stories/D8C2 C9800.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

14. *August 18, Associated Press* — **Anthrax kills hundreds of cattle in parts of Great Plains.** An anthrax outbreak has killed hundreds of cattle in parts of the Great Plains, forcing quarantines and devastating ranchers who worry how they will recover financially. More than 300 animals in North Dakota have died from anthrax in what officials call the worst outbreak among livestock in state history. In South Dakota, at least 200 cattle have been killed. Two ranches in Texas were quarantined last month after anthrax was found in cattle, horses and deer. Spores that cause anthrax can sit dormant in the ground for as long 100 years, said Charles Stoltenow, an extension veterinarian at North Dakota State University. "It just sits there and waits for the right environmental conditions to come around," he said. "You can't predict it." Unusually wet conditions in June, along with high heat and humidity in July, likely played a factor, veterinarians said. "We've had anthrax before, but not of this magnitude," said Andrew Peterson, a veterinarian at the Enderlin Veterinary Clinic in North Dakota. "It started on July 1 and the reports have been daily since then." North Dakota has quarantined 85 areas, which means those producers cannot sell, butcher, or transport animals. The current outbreak has also affected bison, horses, sheep, llamas, elk, and deer, said Beth Carlson, the deputy state veterinarian in North Dakota.
Source: http://www.usatoday.com/news/nation/2005−08−18−cattle−anthra x_x.htm?POE=NEWISVA

15. *August 18, Anchorage Daily News (AK)* — **Potato blight threatens some Alaskan fields.** Matanuska−Susitna, AK, area potato farmers are fighting an outbreak of late blight. The blight is the same disease that caused the Irish potato famine in the mid−19th century. It can also

affect tomatoes, eggplant, and hot peppers. It was first detected in the Mat−Su in 1995 and again in 1998. But it hadn't been seen since then until it turned up last week in a local farmer's field, said state Agriculture Division Director Larry DeVilbiss. So far, parts of three commercial farms in the Valley have been affected, he said. DeVilbiss said one commercial grower has blight in more than half his field. The other two growers have only small pickup−size spots of infected plants. Late blight is a common problem in the Lower 48, but it's rare in Alaska. The fungus thrives in cool, wet weather and is spread by wind and water. It infects a plant, then produces spores that can spread to other plants. It can also survive in potatoes and re−emerge if replanted. The disease can also cause stored potatoes to rot. The spores can spread quickly −− traveling as far as 80 miles in a day −− and the fungus can wipe out entire fields in less than a week.
Source: http://www.adn.com/news/alaska/story/6829509p−6724776c.html

[Return to top]

Food Sector

16. *August 18, RXPg News* — **Oral vaccine may protect animals against E. coli.** Researchers from Austria and Russia have developed an oral vaccine comprised of bacterial ghosts, or empty bacterial envelopes, which may protect against E. coli in animals and humans. Because the major reservoir for E. coli is cattle, researchers are focusing on a vaccine that will prevent infection in both humans and animals. In order to mimic the bacteria's natural route of infection they developed an oral vaccine in hopes of eliciting local immunity in the gut. An oral vaccine containing the bacterial ghosts was administered to mice that were challenged with a lethal dose of the E. coli strain 55 days later. A single dose of the vaccine resulted in an 86 percent protection rate and mice receiving a booster after 28 days showed a 93 percent survival rate. Non−immunized mice challenged with the bacteria had a 26 to 30 percent rate of survival.
Source: http://www.rxpgnews.com/article_2091.shtml

17. *August 18, Guardian (United Kingdom)* — **Bovine Spongiform Encephalopathy transmitted between sheep.** Bovine Spongiform Encephalopathy (BSE) has been transmitted naturally between sheep for the first time. Confirmation that such a thing is possible reinforces fears that the disease may have entered sheep as well as cattle on farms in Britain. Lambs at a government experimental station appear to have caught BSE from their mothers. Their mothers had shown no outward signs of the disease at lambing, one showing them 73 days after lambing, and the other 198 days after. But it is still not certain that the lambs were infected while in the uterus, or shortly before or after lambing. The disease may have spread through the birthing fluids or in some other way. The evidence so far suggests this is far more likely than the lambs catching the disease from other apparently unaffected sheep. Scientists will now seek to estimate from ongoing experiments whether there was ever enough infection in flocks to make the disease survive for long. No evidence of BSE has emerged from testing sheep in abattoirs or on farms. Safety advisers have previously warned that any sheep with BSE entering the food chain would be potentially far more dangerous than a single cow, since there are far more parts of the animal that can carry infection.
Source: http://www.guardian.co.uk/bse/article/0,2763,1550343,00.html ?gusrc=rss

18.

August 17, Associated Press — **Testing options for mad cow said limited.** The U.S. Department of Agriculture (USDA) acknowledged Wednesday, August 17, that its testing options for mad cow disease were limited in 9,200 cases despite its effort to expand surveillance throughout the U.S. herd. In those cases, only one type of test was used −− one that failed to detect the disease in an infected Texas cow. Conducted over the past 14 months, the tests have not been included in the USDA's running tally of mad cow disease tests since last summer. That total reached 439,126 on Wednesday. These 9,200 cases were different because brain tissue samples were preserved with formalin, which makes them suitable for only one type of test −− immunohistochemistry (IHC). In the Texas case, officials had declared the cow free of disease in November after an IHC test came back negative. The USDA's inspector general ordered an additional kind of test, which confirmed the animal was infected. Veterinarians in remote locations have used the preservative on tissue to keep it from degrading on its way to the USDA's laboratory in Ames, IA. Officials this year asked veterinarians to stop using preservative and send fresh or chilled samples within 48 hours.
Source: http://news.yahoo.com/s/ap/20050818/ap_on_go_ot/mad_cow;_ylt=AqiK2OhmI2oTGCpHLqa_lPxZ24cA;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

19. *August 18, Standard (Hong Kong)* — **Antibiotics link to pig disease spread.** The misuse of antibiotics and poor hygiene on mainland pig farms could be the cause of spreading Streptococcus suis infections in China, according to a leading Hong Kong microbiologist. Former Hong Kong Medical Association president Lo Wing−lok said the misuse of antibiotics creates resistance to the same bacteria the drugs are intended to combat. Hong Kong Pig Farm Association chairman Wong Kwong−wing, also a consultant for farmers in Fujian province, said mainland farmers have been feeding pigs antibiotics for at least five or six years. Wong said mainland farmers gave their pigs as many as 10 types of vaccinations. To make matters worse, some even created their own vaccines from tissue samples taken from sick pigs. "This practice is very common on the mainland. It might seem to be an effective method of keeping pigs healthy. However, in fact, it leads to mutation of bacteria and viruses," Wong said. He said nearly 50 percent of mainland pigs die from diseases resulting from the abuse of antibiotics and vaccinations. World Health Organization (WHO) spokesperson for the Western Pacific, Peter Cordingly, said that the WHO would likely investigate whether antibiotic misuse was contributing to the disease.
Source: http://www.thestandard.com.hk/stdn/std/Front_Page/GH18Aa01.h tml

20. *August 17, Associated Press* — **Experts discuss possible bird flu spread in Europe.** As bird flu spreads west across Russia toward Europe, health experts expressed optimism Wednesday,

August 17, that European countries could stamp it out before the virus takes hold and spreads among people. "Will this make its way to Western Europe? I think most of us have no doubt," said Michael Osterholm, an expert on bird flu and director of the Center for Infectious Disease Research and Policy at the University of Minnesota. But he and other experts say that while the situation is worrisome, Europe is better equipped than Southeast Asia to quickly attack the disease that scientists fear could unleash a pandemic. A bird flu outbreak in Europe would be detected more quickly than in Asia, said Juan Lubroth, an animal health expert with the Food and Agriculture Organization, one of the agencies responsible for tracking the virus. And, people don't live in close quarters with animals, as they do in much of Southeast Asia, he said. The European poultry industry also is better able to shelter its birds from contact with the wild ducks blamed for the disease's spread. Experts noted the health care system is better able to deal with human exposure to bird flu and other animal−produced diseases.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/08/17/AR2005081701260.html

21. *August 17, University of California−Riverside* — **Researchers discover model organism for studying viruses.** Researchers at the University of California−Riverside (UCR) have discovered that the worm, C. elegans, makes an excellent experimental host for studying some of the most virulent viruses that infect humans. For years researchers throughout the world have studied C. elegans because many aspects of its biology mirror the biology of humans. However, no viruses were known to infect the millimeter−long roundworm so it was not used as a model for studying viral infections. UCR researchers have developed a strain of the worm, C. elegans, in which an animal virus could replicate, allowing them to map the action and reaction between virus and host. Virus replication in the worm triggers an antiviral response known as RNA silencing or RNA interference (RNAi). RNAi specifically breaks down the virus' RNA. Virus RNA creates proteins that allow the virus to function. The virus responds by producing a protein acting as a suppressor of RNAi to shut down the host's antiviral response. Virus infection did not occur when the viral RNAi suppressor was made inactive by genetic mutations in the host system. C. elegans' RNAi system is considered a "blanket system," meaning that it has parallels in humans, making the worm model a valuable tool in studying the way viruses interact with hosts.
Source: http://www.newsroom.ucr.edu/cgi−bin/display.cgi?id=1141

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

22. *August 18, Island Packet Online (SC)* — **New system to reverse emergency response roles in South Carolina.** Beaufort County, SC, officials soon will be able to alert thousands of residents of an emergency with the simple click of the mouse. Thanks to a $75,172 federal grant that was formally distributed this week, Beaufort County will purchase and put in place an automated

emergency notification system that will allow the county to alert residents of law enforcement emergencies, hazardous materials spills and evacuation notices by telephone. The grant will cover the cost of buying and installing the system. The system, which will be operated by Beaufort County and the Town of Hilton Head Island, SC, will serve the entire county and will be available for use by police, fire departments and the military, among others. "This is the best way to reach the largest amount of people in the shortest period of time," said Beaufort County Sheriff P.J. Tanner. To use the program, officials first target a notification area −− which can be customized down to a city block or span the entire county. Once the area is designated, the program's software cross references the addresses with the 911 database, which includes all landline phone numbers located within the area, including unlisted numbers.
Source: http://www.islandpacket.com/news/local/story/5110622p−465322 4c.html

23. *August 18, Kansas City Star (MO)* — **Disaster teams test themselves in Missouri.** Disaster management officials gathered Wednesday, August 17, at Kansas City, MO's, emergency operations center to test their ability to handle what organizers termed “a cascading series of events” topped off by terrorists exploding a bomb packed with radioactive material at Missouri's Kauffman Stadium. The simulation, which included disaster management teams in St. Louis, MO, and Jefferson City, MO, also involved two bomb attacks in St. Louis and the crash of a truck carrying toxic chemicals on Interstate−70 just east of downtown Kansas City. One of the first lessons organizers learned was the limitations of the virtual tracking system at the emergency operations center. The system is supposed to allow tracking of multiple events and agency responses. “We found that events were happening so hard and furious and were so extensive because of the scenario that it had a difficult time keeping track of everything that was happening,” stated D.A. Christian, Kansas City’s director of emergency management and security. Ultimately, the event tested the ability of officials to communicate, to deploy appropriate resources in the right places and to respond effectively as the problems mounted.
Source: http://www.kansascity.com/mld/kansascity/news/local/12409898 .htm

24. *August 18, Richmond Times−Dispatch (VA)* — **Virginia officials tout use of mobile command center in terrorism fight.** Public safety officials showcased Chesterfield County, VA's, newest crime, rescue and firefighting tool Wednesday, August 17. The county has a new 40−foot−long, $509,000 mobile command center equipped with digital satellite television and Internet service, a weather station, seven computer stations, a telescoping camera with night vision and three television monitors, including a 42−inch plasma screen. Colonel Carl R. Baker, as Chesterfield's police chief emphasized the vehicle's potential role in responding to terrorism related crimes. Because terrorist acts are inherently local crimes, Baker explained, governments at all levels must work together. The new command center is an example of such a partnership with the federal government. "From gathering and sorting intelligence, to communicating with all first responders and all federal agencies, this center can do it all," stated Baker. Chesterfield's police, fire and emergency medical services will share the new vehicle, depending on need. It will be used as a command post from which public safety officials can manage a variety of emergency operations.
Source: http://www.timesdispatch.com/servlet/Satellite?pagename=RTD/MGArticle/RTD_BasicArticle&c=MGArticle&cid=1031784504011

25. *August 18, The Periscope (GA)* — **Emergency drill in Georgia to test Department of Defense emergency response with federal, state and local response agencies.** Beginning

Monday, August 22 and running through Friday, August 26, 1,800 base personnel will participate in a weapons−of−mass−destruction drill (WMD) at the Naval Submarine Base in Kings Bay, GA. The Defense Threat Reduction Agency (DTRA), whose mission is to reduce and counter WMD to maintain national security, will sponsor Dingo King to evaluate and improve the integration of the Department of Defense emergency response with federal, state and local response agencies along with initial notification, procedures command and control and the interaction between the local government and the base. "Our main goal is to refine the base's skills to know what to do in case of an emergency," said Jeff Danshaw, Dingo King program manager. In addition, this exercise provides the first opportunity to evaluate an agreement between Kings Bay, Camden County, Kingsland, St. Marys and Woodbine based upon the Military−Civilian Task Force for Emergency Response Charter, which calls for the development and execution of mutual aid agreements, formal exercises, training and public safety between the base, local governments and the Southeast Georgia Health Care System−Camden Campus.
Source: http://www.kingsbayperiscope.com/stories/081805/kin_dingokin g001.shtml

[Return to top]

Information Technology and Telecommunications Sector

26. *August 17, FrSIRT* — **Microsoft Internet Explorer "Msdds.dll" remote code execution.** A critical vulnerability was identified in Microsoft Internet Explorer, which could be exploited by remote attackers to execute arbitrary commands. This issue is due to a memory corruption error when instantiating the "Msdds.dll" (Microsoft Design Tools Diagram Surface) object as an ActiveX control, which could be exploited by an attacker to take complete control of an affected system via a specially crafted Web page. This vulnerability has been confirmed with Microsoft Internet Explorer 6 SP2 on Windows XP SP2 (fully patched). Note: It is currently unclear whether the "Msdds.dll" library is installed with Microsoft Office, Microsoft Visual Studio, or with other applications. More information will be provided when further details are available. Products affected are: Microsoft Internet Explorer 6 for Microsoft Windows XP SP2; Microsoft Internet Explorer 6 for Microsoft Windows XP SP1; Microsoft Visual Studio .NET 2003; and Microsoft Visual Studio .NET 2002. The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2005/1450

27. *August 17, SecurityFocus* — **WinFTP Server Log−SCR buffer overflow vulnerability.** WinFTP Server is affected by a buffer overflow vulnerability. This issue is due to a failure in the application to do proper bounds checking on user−supplied data. A successful attack can result in overflowing a finite sized buffer and may ultimately lead to arbitrary code execution in the context of the affected application. Security Focus is not currently aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/14581/references

28. *August 17, Security Focus* — **EMC Legato Networker multiple vulnerabilities.** EMC Legato Networker is affected by multiple denial of service, privilege escalation, unauthorized access and arbitrary command execution vulnerabilities. Several vulnerabilities affect EMC Legato Networker which can be exploited to cause denial of service, privilege escalation, unauthorized

access and information disclosure. EMC has released patches addressing these issues: http://www.legato.com/support/websupport/patches_updates/net worker_sec urity_hotfix.htm
Source: http://www.securityfocus.com/bid/14582/references

29. *August 17, FrSIRT* — **phpPgAds SQL injection and command execution vulnerabilities.** Multiple vulnerabilities were identified in phpPgAds, which could be exploited by remote attackers to execute arbitrary commands. The first issue is due to an input validation error in the XML−RPC library when processing, via an "eval()" call, certain XML tags nested in parsed documents, which could be exploited by remote attackers to execute arbitrary PHP commands. For additional information, see : FrSIRT/ADV−2005−1413 The second vulnerability is due to an input validation error in "lib−view−direct.inc.php" when processing a specially crafted "clientid" variable, which could be exploited by malicious users to conduct SQL injection attacks. The third flaw is due to an input validation error when processing specially crafted parameters, which may be exploited by remote attackers to include malicious files and execute arbitrary commands with the privileges of the web server. Products affected are phpPgAds versions prior to 2.0.6.
Users should upgrade to phpPgAds version 2.0.6 :
http://prdownloads.sourceforge.net/phpadsnew/
Source: http://www.frsirt.com/english/advisories/2005/1447

30. *August 16, Security Focus* — **BlueZ Arbitrary command execution vulnerability.** The vendor has addressed this issue in version 2.19: BlueZ is affected by an arbitrary command execution vulnerability. This issue is due to a failure in the application to properly sanitize user−supplied input. Successful exploitation of this vulnerability will permit an attacker to execute arbitrary commands on the system hosting the affected application in the security context of the application. This may aid in further attacks against the underlying system; other attacks are also possible. The vendor has addressed this issue in version 2.19.
Source: http://www.securityfocus.com/bid/14572/info

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT has seen reports of multiple families of malicious code that take advantage of the vulnerability described in VU#998653 (MS05−039). This includes, but is not limited to, several variants of the Zotob worm and other malware including the W32/Rbot and W32/SDBot families of malicious code.

The malware scans for vulnerable systems on port 445/tcp. Upon infection a compromised host will attempt to scan and exploit other systems at randomly generated IP addresses. The functionality has evolved within the Zotob family and

with the addition of other malware families; the scope of attack may expand to include:

* Spyware functionality (key logging, video, audio screen captures)
* Data theft (authentication credentials, CD Keys to popular applications)
* Mass mailing

While the primary attack target is the Plug and Play vulnerability on Windows 2000 systems, Windows XP and Windows Server 2003 are also exposed to the Plug and Play vulnerability under more limited circumstances. For information on these circumstances, please refer to the "Mitigating Factors" section of the Microsoft Security Advisory.

Once a system is compromised with any of the above listed malicious code, additional vulnerabilities may be exploited across multiple operating systems (including Windows XP and Server 2003) to get malicious code installed on a system.

More information on the vulnerability is available in the following US−CERT Vulnerability Note:

VU#998653 − Microsoft Plug and Play contains a buffer overflow vulnerability

Microsoft has published a Security Advisory that provides guidance on Zotob and its variants. For more information, please see URL:

http://www.microsoft.com/technet/security/advisory/899588.ms px

Microsoft has also published some additional information concerning Zotob and what actions users can take now. For more information, please review URL: http://www.microsoft.com/security/incident/zotob.mspx

US−CERT urges users to apply the update described in Microsoft Security Bulletin MS05−039. If users are unable to apply the update, Microsoft provides several workarounds that may help to protect against known attacks on this vulnerability. For more information on computer viruses, please refer to our Computer Virus Resources document.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 1026 (−−−), 6881 (bittorrent), 1433 (ms−sql−s), 135 (epmap), 139 (netbios−ssn), 6346 (gnutella−svc), 1234 (hotline), 1434 (ms−sql−m), 15901 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

31. *August 18, Honolulu Advertiser (HI)* — **Businesses lagging in disaster readiness.** Hawaii businesses lack continuity plans and are generally less prepared for a disaster than businesses on the West Coast, according to a survey by AT&T and the International Association of Emergency Managers. Six of 14 Hawaii companies surveyed said they do not have a continuity plan in place and half said they do not consider continuity planning a priority. Some 45 percent of the companies surveyed established redundant servers and/or backup sites to ensure continuity of operations during a disaster. But only three of 14 Hawaii companies established redundant servers and/or backup sites. The survey was based on 100 telephone interviews conducted May 19 through June 14 by Opinion Research Corp. The businesses were located in Hawaii, Alaska, Oregon and California, excluding Los Angeles. The survey's results surprised city and state civil defense officials, who said continuity planning is one of the key parts of their disaster preparedness materials and messages to businesses. A brochure that state civil defense officials sent to every Hawaii business about a year ago urges businesses to review their emergency plans, including continuity of operations.
Source: http://the.honoluluadvertiser.com/article/2005/Aug/17/bz/FP5 08170321.html

32. *August 17, San Bernadino Sun News (CA)* — **California district readies for disasters.** A special federal grant totaling nearly a quarter of a million dollars will help ensure that the Rialto, CA, Unified School District is well prepared in an emergency, both in training and technology. The $241,000 grant, awarded last fall, is being used to pay for special training to teach district employees how to cope with disasters, said Jerry Sturmer, director of educational safety and security for the district. "In an emergency we could be on our own for up to 72 hours," Sturmer said. "My goal is to get enough school personnel trained so that in case of a disaster teachers, custodians, secretaries would be drafted into service as rescue and aid workers," he continued. So far, more than 100 employees have been certified, which includes training in how to do light search and rescue, triage and putting out small fires. The district also is using the grant to purchase special geographic information systems software, Sturmer said. The district recently installed a live GIS system that keeps track of its buses and security vehicles at all times.
Source: http://www.sbsun.com/Stories/0,1413,208~12588~3013004,00.htm l

[Return to top]

General Sector

33. *August 18, Associated Press* — **Greece faces pressure on plane crash info.** The Greek government came under increasing pressure Thursday, August 18, to release information about the crash of a Cypriot plane last week, as rumors swirled surrounding the disaster that left all 121 people aboard dead. Investigators, meanwhile, had recovered the main components of the wreckage of the Helios Airways Boeing 737−000 and would begin examining them Thursday, said chief investigator Akrivos Tsolakis. In London, the British Airline Pilots' Association on Wednesday urged Greek authorities to release preliminary findings. “There have been several

apparently conflicting reports and a number of statements that just don't add up," said union head Captain Melvyn Granshaw, without elaborating. "There is a concern in our industry to learn, as quickly as possible, what happened." The government has consistently said the cause of the crash was likely technical failure, not terrorism. But industry experts say that with so many unanswered questions, it was too soon to tell.
Source: http://www.guardian.co.uk/worldlatest/story/0,1280,−5218672, 00.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer